AMENDMENTS to the CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (currently amended) A system for authenticating a client device requesting a session of service from a service provider, comprising:

a first ~~at least two matching~~ one-time pad cryptological table ~~tables, a first of which is stored in a client device, and a second of which is~~ accessible by a cellular telephone service security server, ~~each~~ said first table having multiple entries, each entry including a field for [[a]] an indicator of previous use, said previous use indicator for each entry being initialized in an "unused" state, each [[row]] entry containing at least one One Time Pad value;

a second one-time pad cryptological table stored in an authentic cellular telephone device, initially synchronized with said multiple entries, fields, and indicators of previous use of said first one-time pad cryptological table;

a first copy of said second one-time pad cryptological table stored in a cloned inauthentic cellular telephone device, said first copy being initially synchronized with said multiple entries, fields, and indicators of previous use of said second one-time pad cryptological table;

a code transmitter portion of said authentic cellular telephone device configured to select an unused entry in said second one-time pad cryptological table, and to transmit said selected entry to a telephone network upon requesting initiation of a service session;

a code exchanger portion of said cellular telephone service security server configured to receive a One Time Pad [[pad]] value from said authentic cellular telephone ~~client~~ device and from said cloned inauthentic cellular telephone device ~~by said service security server~~ upon request for initiation of a service session;

a code comparator portion of said cellular telephone service security server configured to determine [[if]] that said received One Time Pad value is marked as "used" or "unused" in said ~~second~~ first one-time pad cryptological table;

a service session grantor configured to grant said service request responsive to determination that said received One Time Pad value is unused, including changing said used indicator to a "used" state in said first one-time pad

cryptological table upon said grant of service, and further configured to disable service to said cloned inauthentic cellular telephone device responsive to determining that said first one-time pad cryptological table is not synchronized with said first copy of said second one-time pad cryptological table; and

a table updater portion of said authentic cellular telephone device configured to, responsive to granting of sais service request, mark said transmitted One Time Pad as "used", wherein said first one-time pad crytological table and said second one-time pad cryptological tables are kept in synchronization.

~~a client device reconfiguratorconfigured to challenge said user of said client device responsive to determining that said received One Time Pad value is marked as "used", and to replace said first and second tables with new, synchronized tables responsive to successful response by said user to said challenge, completing authentication of said client device without the need for a service history counter.~~

2. (currently amended) The system as set forth in Claim 1 wherein:

said one-time pad cryptological tables further comprise a sequence index;

said code comparator is further configured to determine if said received One Time Pad value is a next unused pad according to said sequence indicators; and

said session grantor is configured to grant a session only if said received pad is a next expected One Time Pad value, [[; and]]

~~said client device reconfigurator is configured to respond to said received One Time Pad value not being a next expected One Time Pad value.~~

Claims 3 - 4 (cancelled).

5. (previously presented) The system as set forth in Claim 1 wherein:

said one-time pad cryptological tables further comprise an expiration field for each entry;

said code comparator is further configured to determine if said received pad is expired;

said session grantor is configured to grant a session only if said received pad is unexpired; and

said client device reconfigurator is ~~adapted~~ configured to respond to said received pad being expired.

6. (cancelled)

7. (previously presented) The system as set forth in Claim 1 wherein said service session grantor is further configured to require a second step of acknowledgment between said service security server and said client device before said entry is marked as "used".

8. (currently amended) A method for authenticating a client device requesting a session of service from a service provider, said method comprising the steps of:

providing a first ~~at least two matching~~ one-time pad cryptological table ~~tables, disposing a first of which in a client device, and disposing a second of which such that it is~~ accessible by a cellular telephone service security server, [[each]] said table having multiple entries, each entry including a field for an indicator of previous use, said previous use indicator for each entry being initialized in an "unused" state, each [[row]] entry containing at least one One Time Pad value;

providing a second one-time pad cryptological table stored in an authentic cellular telephone device, initially synchronized with said multiple entries, fields, and indicators of previous use of said first one-time pad cryptological table;

providing a first copy of said second one-time pad cryptological table stored in a cloned inauthentic cellular telephone device, said first copy being initially synchronized with said multiple entries, fields, and indicators of previous use of said second one-time pad cryptological table;

selecting by a portion of said authentic cellular telephone device an unused entry in said second one-time pad cryptological table, and transmitting said selected entry to a telephone network upon requesting initiation of a service session;

receiving by a portion of said cellular telephone service security server a One Time Pad value from said authentic cellular telephone device or from said inauthentic clone cellular telephone device ~~client device by said service security server upon request for initiation of a service session~~;

determining by a portion of said cellular telephone service security server if said received One Time Pad value is marked as "used" or "unused" in said ~~second~~ first one-time pad cryptological table;

responsive to determination that said received One Time Pad value is unused, granting said service request and changing said used indicator corresponding to said One Time Pad entry in said first one-time pad cryptological ~~second~~ table to a "used" state; and

responsive to determining that said received One Time Pad value is marked as "used" in said first one-time pad cryptological table, disabling service to said cloned

inauthentic cellular telephone device ~~, challenging said user of said client device, and replacing said first and second tables with new, synchronized tables responsive to successful response by said user to said challenge, completing~~ wherein authentication of said ~~client~~ authentic cellular telephone device is completed without [[the]] need for a service history counter.

9. (currently amended) The method as set forth in Claim 8 wherein:

said ~~step of providing~~ one-time pad cryptological tables further comprise ~~comprises~~ providing a sequence index field for each table entry;

~~said step of~~ determining [[if]] that said received One Time Pad value is used comprises determining [[if]] that said received One Time Pad is a next unused One Time Pad value according to said sequence indicators; and

said ~~step of~~ granting ~~a session~~ comprises granting a session responsive to ~~only if~~ said received One Time Pad value being [[is]] a next expected pad value, [[; and]]

~~said step of challenging said user comprises challenging said user responsive to said received One Time Pad value not being a next expected pad value.~~

10. (cancelled)

11. (currently amended) The method as set forth in Claim [[8]] 9 wherein said ~~step of~~ challenging a user comprises challenging a user with one or more methods selected from [[the]] a group comprising [[of]] requiring a user name input, requiring a password input, requiring an account number input, requiring an answer to a secret question, and requiring a user-designated response.

12. (currently amended) The method as set forth in Claim 8 wherein:

~~said step of~~ providing one-time pad cryptological tables further comprises providing an expiration field for each entry;

~~said step of~~ determining [[if]] that said received One Time Pad comprises determining [[if]] that said received One Time Pad is expired;

~~said step of~~ granting a session comprises granting a session only responsive to [[if]] said received One Time Pad is unexpired; and

~~said step of~~ challenging a user and replacing said tables comprises challenging a user [[if]] responsive to said received pad [[is]] being determined to be expired.

Claims 13 - 14. (cancelled)

15. (currently amended) An article of manufacture for authenticating a client device requesting a session of service from a service provider, comprising:

a computer readable medium suitable for encoding one or more software programs; and

one or more software programs configured to cause a processor to perform the steps of:

providing a first ~~at least two matching~~ one-time pad cryptological table ~~tables, disposing a first of which in a client device, and disposing a second of which such that it is~~ accessible by a cellular telephone service security server, [[each]] said table having multiple entries, each entry including a field for an indicator of previous use, said previous use indicator for each entry being initialized in an "unused" state, each [[row]] entry containing at least one One Time Pad value;

providing a second one-time pad cryptological table stored in an authentic cellular telephone device, initially synchronized with said multiple entries, fields, and indicators of previous use of said first one-time pad cryptological table;

providing a first copy of said second one-time pad cryptological table stored in a cloned inauthentic cellular telephone device, said first copy being initially synchronized with said multiple entries, fields, and indicators of previous use of said second one-time pad cryptological table;

selecting by a portion of said authentic cellular telephone device an unused entry in said second one-time pad cryptological table, and transmitting said selected entry to a telephone network upon requesting initiation of a service session;

receiving by a portion of said cellular telephone service security server a One Time Pad value from said authentic cellular telephone device or from said inauthentic clone cellular telephone device ~~client device by said service security server upon request for initiation of a service session~~;

determining by a portion of said cellular telephone service security server if said received One Time Pad value is marked as "used" or "unused" in said ~~second~~ first one-time pad cryptological table;

responsive to determination that said received One Time Pad value is unused, granting said service request and changing said used indicator

corresponding to said One Time Pad entry in said first one-time pad cryptological ~~second~~ table to a "used" state; and

responsive to determining that said received One Time Pad value is marked as "used" in said first one-time pad cryptological table, disabling service to said cloned inauthentic cellular telephone device ~~, challenging said user of said client device, and replacing said first and second tables with new, synchronized tables responsive to successful response by said user to said challenge, completing~~ wherein authentication of said ~~client~~ authentic cellular telephone device is completed without [[the]] need for a service history counter.

16. (currently amended) The article as set forth in Claim 15 wherein:

said software for providing one-time pad cryptological tables further comprises software configured to provide ~~for providing~~ a sequence index field for each table entry;

said software for determining [[if]] that said received One Time Pad value is used comprises software configured to determine that ~~for determining if~~ said received pad is a next unused pad value according to said sequence indicators; and

said software for granting a session comprises software configured to grant ~~for granting~~ a session only [[if]] responsive to said received pad value [[is]] being a next expected pad value . [[; and]]

~~said software for challenging said user comprises software for challenging said user responsive to said received pad value not being a next expected pad value.~~

Claim 17 (cancelled).

18. (currently amended) The article as set forth in Claim 15 further comprising ~~wherein said~~ software configured to challenge ~~for challenging a user comprises software for challenging~~ a user with one or more methods selected from [[the]] a group [[of]] comprising requiring a user name input, requiring a password input, requiring an account number input, requiring an answer to a secret question, and requiring a user-designated response.

19. (currently amended) The article as set forth in Claim 15 wherein:

said software for providing one-time pad cryptological tables further comprises software configured to provide ~~for providing~~ an expiration field for each entry;

said software for determining [[if]] that said received One Time Pad comprises

software configured to determine that ~~for determining if~~ said received One Time Pad is expired;

said software for granting a session comprises software configured to grant ~~for granting~~ a session only responsive to [[if]] said received One Time Pad [[is]] being unexpired; and

said software for challenging a user and replacing said tables comprises software configured to challenge ~~for challenging~~ a user responsive to [[if]] said received One Time Pad being [[is]] determined to be expired.

Claims 20 - 21 (cancelled)